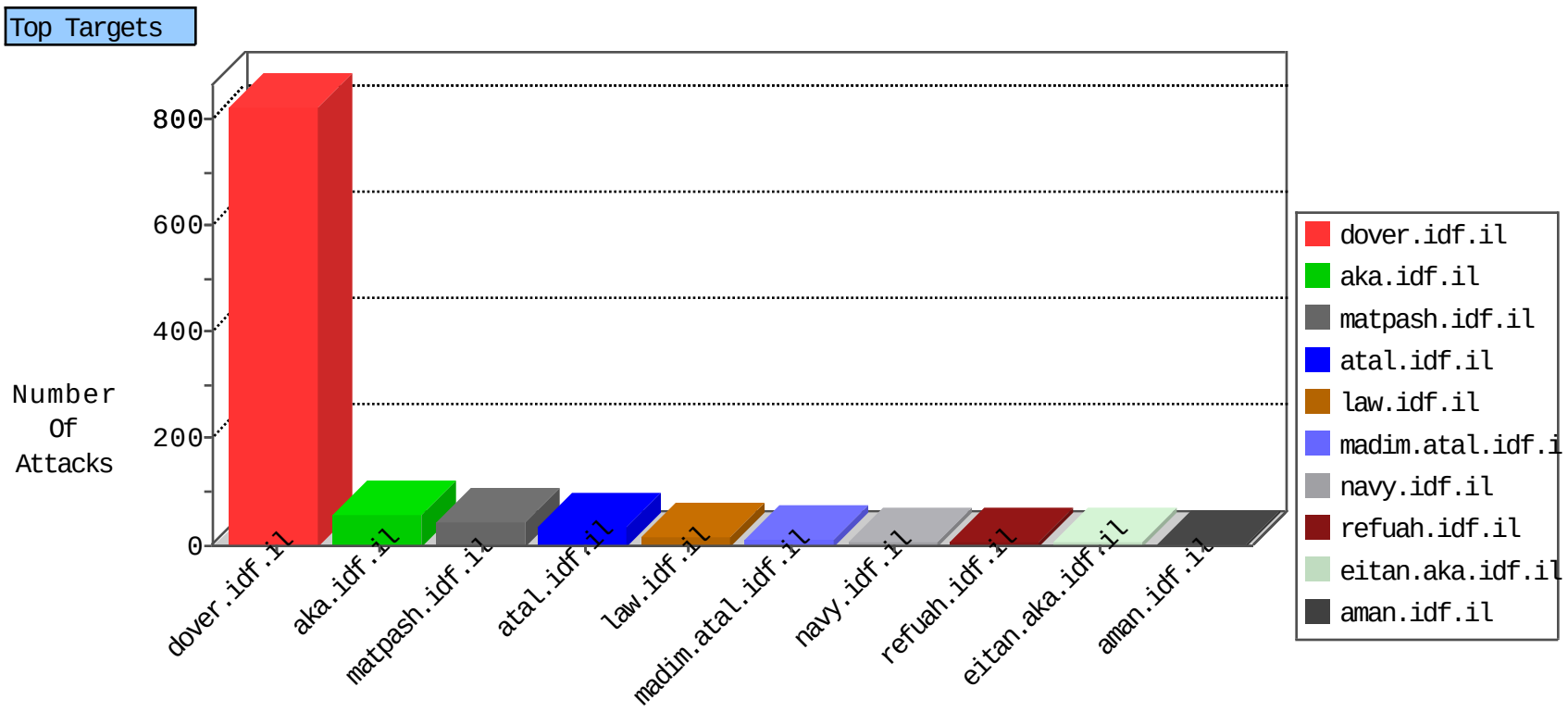
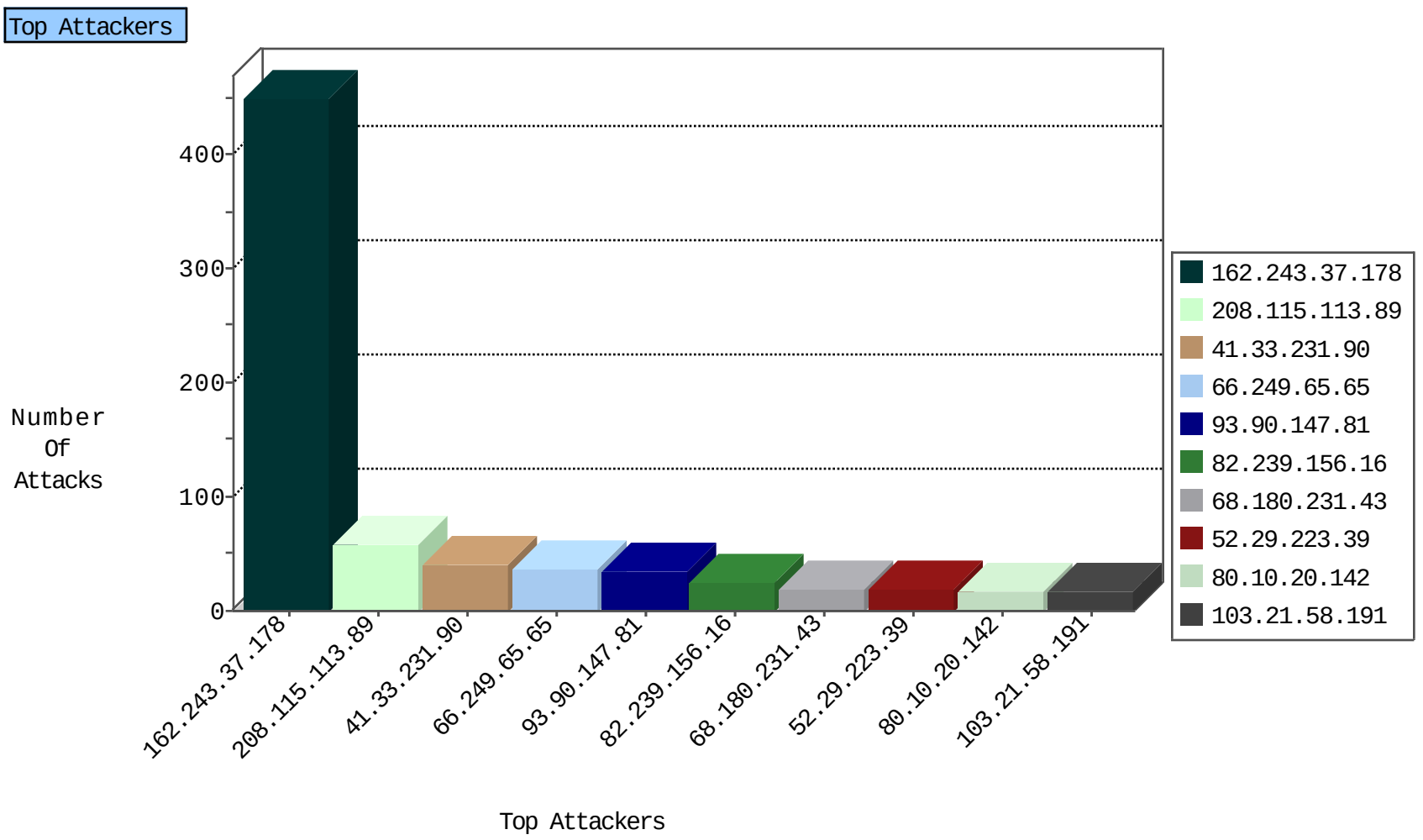
04-22-2016-07:04:01 to 04-22-2016-08:04:01

IDF Under Attack
Daily Report





04-22-2016-07:04:01 to 04-22-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.58.51.159	Uruguay	147.237.8.45	e.eitan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
66.184.132.24	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-22-2016-07:04:01 to 04-22-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
103.21.58.191	India	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-22-2016-07:04:01 to 04-22-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.90.147.81	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	22
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
81.169.171.4	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -sS window 2048	1
210.117.121.60	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.208	147.237.76.200	Lithuania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.214.73.227	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.139	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.208	147.237.77.243	Lithuania	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.208	147.237.8.50	Lithuania	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

04-22-2016-07:04:01 to 04-22-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.243.37.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	450
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
82.239.156.16	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	25
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.10.20.142	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
107.167.99.226	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.222.28.91	Tanzania, United Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.239.6.57	Uganda	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.99.32.7	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.8.239.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.130.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.217.177	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
66.184.132.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
123.2.236.33	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.184.132.24	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.61.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.130.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
119.30.32.38	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
24.107.122.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
65.55.210.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.60	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.178.18	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.58.51.159	Uruguay	147.237.0.35	akaws.idf.il	drop		drop	1

04-22-2016-07:04:01 to 04-22-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	11
217.132.158.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
79.181.62.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.226.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.85	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding jw]ba3d*)B*{kHfBEqAPKgV2cp^2doa5W[ySI(.xy*a3uHovmpZ6hYByFMm{MiyX.;S;!_Mw[2crof_CD-b*NLD1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.253.226.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
199.249.233.131	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/mobile	Block	1
91.109.30.73	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
220.255.98.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
110.53.183.62	China	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/pniot.aspx	Block	1
207.46.13.73	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
92.241.41.106	Jordan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
40.77.167.87	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
220.255.146.215	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
119.30.32.38	Bangladesh	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	1
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
207.46.13.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.123.171.215	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14615-he/	Block	1
66.249.64.176	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in eitan.aka.idf.il/938-en/eitan.aspx	None	1
220.255.148.142	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1

04-22-2016-07:04:01 to 04-22-2016-08:04:01